**Приложение № 2**

к Договору оферты «Условия обслуживания физических лиц

в Банке РМП (ПАО) с использованием Системы ДБО»

**ИНСТРУКЦИЯ**

**по обеспечению информационной безопасности при работе Клиента**

**в Системе дистанционного банковского обслуживания физических лиц в Банке РМП (ПАО)**

1. **Общие положения**
	1. Использование средств дистанционного банковского обслуживания всегда связано с повышенными рисками потери денежных средств, поэтому Вы обязаны ознакомиться с настоящей Инструкцией до начала работы в Системе ДБО.
	2. При работе в Системе ДБО используются следующие средства защиты:

**1.2.1.** **Защищенное соединение с Банком**.

Признаком установки защищенного соединения является наличие информации о протоколе **https** в адресной строке используемого клиентом браузера

[**https://elf.faktura.ru/elf/app/?site=rmp**](https://elf.faktura.ru/elf/app/?site=rmp)

При входе в Систему ДБО всегда проверяйте указанный адрес.

**1.2.2.** **Средства подтверждения**.

Одноразовые пароли используются при входе в Систему ДБО и проведении операций в Системе ДБО. Одноразовые пароли направляются SMS-сообщением/PUSH-уведомлением на Ваш телефон, указанный в Заявлении об акцепте оферты «Условия обслуживания физических лиц в Банке РМП (ПАО) с использованием Системы ДБО» (далее – Заявление об акцепте оферты).

После ввода Логина и Пароля для входа в Систему ДБО, Система ДБО потребует от Вас ввести Одноразовый пароль.

После ввода всех данных для перевода денежных средств Система ДБО предложит Вам ввести Одноразовый пароль с целью подтверждения операции.

Одноразовый пароль должен быть введен Вами в течение 120 секунд. Если в течение указанного времени Одноразовый пароль не был введен, он становится недействительным. В этом случае Вам необходимо получить новое SMS-сообщение/PUSH-уведомление с новым Одноразовым паролем.

1. **Требования к информационной безопасности при работе в Системе ДБО**
	1. Используйте только лицензионную операционную систему на Вашем компьютере.
	2. Своевременно устанавливайте обновления операционной системы и прикладных программ, рекомендуемые разработчиком программного обеспечения. Копируйте обновления только с официальных сайтов разработчиков программного обеспечения.
	3. Используйте дополнительные средства безопасности программного обеспечения – антивирусные программы, программы защиты от спам-рассылок и пр.

Используйте только современное, лицензионное антивирусное программное обеспечение.

* 1. Если у Вас есть подозрение, что Ваше **Средство идентификации (Логин)** или **Средство аутентификации (Пароль) скомпрометированы, т.е. стали известны третьим лицам**, либо произошло несанкционированное списание денежных средств со Счета:
		1. Незамедлительно выключите компьютер (ноутбук, планшет и т.п.).
		2. Незамедлительно сообщите об инциденте в Центральный офис Банка

**по телефонам**

***+7 (495) 737-86-43, +7 (495) 737-86-44, +7 (499) 967-86-44***

***с понедельника по четверг – с 9.30 до 18.30 (по московскому времени),***

***в пятницу и предпраздничные дни – с 9.30 до 17.15 (по московскому времени).***

Для проведения Банком аутентификации Вам потребуется назвать Кодовое слово, которое Вы указали в Заявлении об акцепте оферты.

После проведения аутентификации Банк незамедлительно осуществит блокировку Вашего Пароля и Идентификатора пользователя для входа в Систему ДБО, а также блокировку возможности проведения через Систему ДБО операций по Вашим счетам/картам, подключенным к Системе ДБО.

* + 1. Если инцидент произошел в нерабочее время Банка, и к Системе ДБО подключен(-ы) Счет(-а), операции по которому(-ым) проводятся с использованием банковских карт, незамедлительно сообщите об инциденте в Процессинговый центр

**по телефону**

***+7(495)232-37-23***

**круглосуточно.**

* + 1. Незамедлительно примите меры для отзыва распоряжений на проведение расходных операций по Вашим счетам/картам, несанкционированных Вами. Для этих целей желательно использовать другой компьютер.

Следует учитывать, что через Систему ДБО распоряжение может быть отозвано Клиентом в день его регистрации в Системе ДБО и только в том случае, если оно не исполнено, и Банк имеет возможность отменить его исполнение.

В других случаях неисполненное Банком распоряжение может быть отозвано (если Банк имеет возможность его отзыва) после Вашего звонка в Центральный офис Банка

**по телефонам**

***+7 (495) 737-86-43, +7 (495) 737-86-44, +7 (499) 967-86-44***

***с понедельника по четверг – с 9.30 до 18.30 (по московскому времени),***

***в пятницу и предпраздничные дни – с 9.30 до 17.15 (по московскому времени).***

Для проведения Банком аутентификации Вам потребуется назвать Кодовое слово, которое Вы указали в Заявлении об акцепте оферты. После проведения аутентификации Банк незамедлительно осуществит блокировку Вашего Пароля и Идентификатора пользователя для входа в Систему ДБО, а также блокировку возможности проведения через Систему ДБО операций по Вашим счетам/картам, подключенным к Системе.

* + 1. **Не позднее 3 (Трех) рабочих дней после обращения в Банк с устным уведомлением об инциденте в обязательном порядке направьте подтверждающее письменное *Уведомление* по форме Приложения № 6 к Договору оферты со своего адреса электронной почты на адрес электронной почты Банка**

**bk@bankrmp.ru**

либо представьте **подтверждающее письменное *Уведомление*****лично в любой офис Банка** (актуальный перечень офисов Банка с адресами и телефонами размещен на сайте [**http://bankrmp.ru**](http://bankrmp.ru/)**)**.

* 1. Если утерян либо похищен телефон (SIM-карта) с номером, указанным в Заявлении об акцепте оферты, незамедлительно сообщите об этом оператору сотовой связи для блокировки SIM-карты.

Затем сообщите об инциденте в Центральный офис Банка

**по телефонам**

***+7 (495) 737-86-43, +7 (495) 737-86-44, +7 (499) 967-86-44***

***с понедельника по четверг – с 9.30 до 18.30 (по московскому времени),***

***в пятницу и предпраздничные дни – с 9.30 до 17.15 (по московскому времени).***

Для проведения Банком аутентификации Вам потребуется назвать Кодовое слово, которое Вы указали в Заявлении об акцепте оферты.

* 1. Никогда и никому (включая сотрудников Банка) не сообщайте Ваш Пароль и Одноразовый пароль.
	2. Не сохраняйте Ваш Пароль и Логин на компьютере либо на других носителях электронной информации.
	3. Внимательно проверяйте текст SMS-сообщения/PUSH-уведомления, которое содержит не только Одноразовый пароль, но и краткую информацию о совершаемой операции.
	4. Никогда не подтверждайте операцию Одноразовым паролем, если информация в SMS-сообщении/ PUSH-уведомлении не совпадает с операцией, которую Вы хотите подтвердить.
	5. Не устанавливайте на мобильный телефон, на который Банк отправляет SMS-сообщения/PUSH-уведомления с Одноразовым паролем, приложения, полученные от неизвестных Вам источников. Банк никогда не рассылает своим клиентам ссылки и указания на установку приложений, за исключением приложений, размещенных самим Банком в официальных магазинах интернет-приложений для Android и Apple. Используйте только официальные приложения Банка, доступные в официальных репозиториях производителей мобильных платформ App Store и Google Play. Обязательно убедитесь, что разработчиком указан Банк РМП (ПАО). При получении такого предложения незамедлительно сообщите об этом в Центральный офис Банка

**по телефонам**

***+7 (495) 737-86-43, +7 (495) 737-86-44, +7 (499) 967-86-44***

***с понедельника по четверг – с 9.30 до 18.30 (по московскому времени),***

***в пятницу и предпраздничные дни – с 9.30 до 17.15 (по московскому времени).***

Для проведения Банком аутентификации Вам потребуется назвать Кодовое слово, которое Вы указали в Заявлении об акцепте оферты.

* 1. Не заходите в Систему ДБО с того же мобильного телефона, устройства, на которое приходят SMS-сообщения Банка с Одноразовым паролем.
	2. По возможности, используйте в качестве устройства для получения SMS - сообщений от Банка простейший мобильный телефон, а не смартфон, поскольку риск заражения смартфона вредоносным программным обеспечением несоизмеримо выше.
	3. Не реже одного раза в день просматривайте выписки об операциях по счетам/картам, подключенным к Системе ДБО.
	4. Для связи с Банком используйте только телефоны, указанные в настоящей Инструкции либо на сайте Банка [**http://bankrmp.ru**](http://bankrmp.ru/).